ABSTRAK

Nama : Kosmas Pria Adi Nagara
Program Studi : Teknik Informatika
Judul : Analisis Keamanan Website LPPM ISTN Menggunakan Metode Pentest

Kemajuan teknologi informasi telah meningkatkan penggunaan website dalam pengelolaan informasi akademik, termasuk pada institusi pendidikan. Namun, meningkatnya penggunaan website juga diiringi dengan ancaman *keamanan siber*, seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan *serangan DDoS*. Penelitian ini bertujuan untuk menguji keamanan website Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) ISTN, menggunakan metode *penetration testing* guna mengidentifikasi kelemahan serta memberikan rekomendasi perbaikan. Pengujian dilakukan menggunakan berbagai alat keamanan, seperti *Nessus* dan *OWASP ZAP*, serta teknik analisis port dan jaringan. Hasil penelitian menunjukkan bahwa website *LPPM ISTN* menggunakan *Web Application Firewall (WAF)* yang cukup efektif dalam menangkal serangan. Namun, ditemukan beberapa kerentanan, seperti DNS Server Spoofed Request Amplification DDoS, potensi Eksploitasi clickjacking, serta beberapa port terbuka yaitu 80, 443, dan 5432 yang dapat dimanfaatkan oleh penyerang. Selain itu, perubahan IP domain utama ISTN juga terdeteksi selama penelitian. Berdasarkan hasil pengujian, direkomendasikan perbaikan pada sistem keamanan, termasuk pembaruan CMS dan PHP, peningkatan kebijakan keamanan konten, serta perbaikan pada sistem DNS dan sertifikat SSL. Penelitian ini diharapkan dapat meningkatkan keamanan *website akademik* dan menjadi referensi bagi pengujian keamanan siber di masa mendatang.

Kata Kunci: *keamanan siber, penetration testing, website akademik, LPPM ISTN, SQL Injection, Cross-Site Scripting (XSS), Serangan DDoS, Web Application Firewall (WAF), OWASP ZAP.*

ABSTRACT

Name : Kosmas Pria Adi Nagara
Study Program : Computer Engineering
Title : LPPM ISTN Website Security Analysis Using the Pentest Method

Advances in information technology have increased the use of websites in academic information management, including in educational institutions. However, this increased use is accompanied by *cybersecurity* threats such as *SQL Injection*, *Cross-Site Scripting (XSS), and DDoS attacks*. This research aims to test the security of the ISTN Institute for Research and Community Service (LPPM) website using the *penetration testing* method to identify vulnerabilities and provide recommendations for improvement. Testing was conducted using various security tools, including Nessus and *OWASP ZAP*, as well as network and port analysis techniques. The results show that the *LPPM ISTN* website uses a *Web Application Firewall (WAF)* which is relatively effective in preventing attacks. However, several vulnerabilities were found, such as DNS Server Spoofed Request Amplification DDoS, potential clickjacking exploits, and open ports which are 80, 443, and 5432 that can be utilized by attackers. In addition, changes in ISTN's main domain IP were also detected during the research. Based on these findings, improvements are recommended, including updating CMS and PHP versions, improving content security policies, and upgrading DNS systems and SSL certificates. This research is expected to improve the security of *academic websites* and become a reference for future cybersecurity testing.

Keywords: cybersecurity, penetration testing, academic websites, LPPM ISTN, SQL Injection, Cross-Site Scripting (XSS), DDoS Attack, Web Application Firewall (WAF), OWASP ZAP.